

JP 01/772 日 本 国 特 許 庁
 EU
 PATENT OFFICE
 JAPANESE GOVERNMENT

#4

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
 Date of Application:

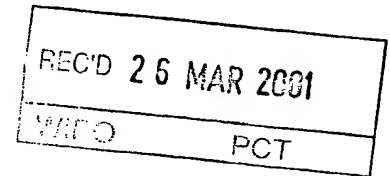
2000年 8月 2日

出 願 番 号
 Application Number:

特願2000-234752

出 願 人
 Applicant(s):

ソニー株式会社



09/937797

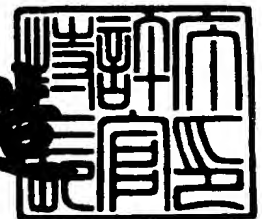
PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
 COMPLIANCE WITH RULE 17.1(a) OR (b)

2001年 3月 2日

特許庁長官
 Commissioner,
 Patent Office

及 川 耕 造



出証番号 出証特2001-3015165

【書類名】 特許願

【整理番号】 0000171203

【提出日】 平成12年 8月 2日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 齋藤 真

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 金巻 裕史

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 佐竹 清

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100094053

 【弁理士】

 【氏名又は名称】 佐藤 隆久

【手数料の表示】

 【予納台帳番号】 014890

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707389

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信装置、通信システムおよびその方法

【特許請求の範囲】

【請求項 1】

利用者を識別するための識別情報を含む要求を受信する受信手段と、
前記識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、
前記要求に応じて所定の処理を行う処理手段と、
前記要求に含まれる前記識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する送信手段と
を有する通信装置。

【請求項 2】

前記受信手段は、暗号化された前記識別情報を含む前記要求を受信し、
前記通信装置は、
前記受信した要求に含まれる前記識別情報を復号する復号手段
をさらに有する請求項 1 に記載の通信装置。

【請求項 3】

前記識別情報は、当該通信装置に登録された利用者に予め割り当てられた識別子である
請求項 1 に記載の通信装置。

【請求項 4】

前記処理の結果を送信する送信先の情報は、前記要求の送信元がオフラインで当該通信装置に提供した情報である
請求項 1 に記載の通信装置。

【請求項 5】

前記所定の結果を送信する送信先の情報は、当該通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための識別情報である
請求項 1 に記載の通信装置。

【請求項 6】

前記処理は、認証処理である
請求項 1 に記載の通信装置。

【請求項 7】

ネットワークを介して接続される第 1 の通信装置および第 2 の通信装置を有する通信システムであって、

前記第 1 の通信装置は、

利用者を識別するための識別情報を含む要求を受信する第 1 の受信手段と、

前記識別情報と処理の結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、

前記要求に応じて所定の処理を行う処理手段と、

前記要求に含まれる前記識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する第 1 の送信手段と

を有し、

前記第 2 の通信装置は、

前記要求を前記第 1 の通信装置に送信する第 2 の送信手段と、

前記処理の結果を前記第 1 の通信装置から受信する第 2 の受信手段と、

当該受信した認証処理の結果を出力する出力手段と

を有する

通信システム。

【請求項 8】

前記第 1 の通信装置の前記第 1 の受信手段は、暗号化された前記識別情報を含む前記要求を受信し、

前記第 1 の通信装置は、

前記受信した要求に含まれる前記識別情報を復号する復号手段

をさらに有する請求項 7 に記載の通信システム。

【請求項 9】

前記識別情報は、当該第 1 の通信装置に登録された利用者に予め割り当てられ

た識別子である

請求項 7 に記載の通信システム。

【請求項 1 0】

前記処理の結果を送信する送信先の情報は、前記第 2 の通信装置の利用者がオフラインで当該第 1 の通信装置に提供した情報である

請求項 7 に記載の通信システム。

【請求項 1 1】

前記処理の結果を送信する送信先の情報は、前記第 1 の通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための識別情報である

請求項 7 に記載のシステム。

【請求項 1 2】

ネットワークを介して接続される第 1 の通信装置および第 2 の通信装置を用いた通信方法であって、

利用者を識別するための識別情報を含む要求を、前記第 2 の通信装置から前記第 1 の通信装置に送信し、

前記第 1 の通信装置において、前記要求に応じて所定の処理を行い、

前記第 1 の通信装置は、予め用意された前記識別情報と処理の結果を送信する送信先の情報とを対応関係を参照し、前記要求に含まれる前記識別情報に対応する送信先の情報によって特定される送信先に、前記処理の結果を送信する

通信方法。

【請求項 1 3】

前記第 2 の通信装置において前記第 1 の通信装置から受信した前記処理の結果を出力する

請求項 1 2 に記載の通信方法。

【請求項 1 4】

前記第 1 の通信装置は、暗号化された前記識別情報を含む前記要求を受信し、当該受信した要求に含まれる前記識別情報を復号する

請求項 1 2 に記載の通信方法。

【請求項 1 5】

前記識別情報は、当該第 1 の通信装置に登録された利用者に予め割り当てられた識別子である

請求項 1 2 に記載の通信方法。

【請求項 1 6】

前記処理の結果を送信する送信先の情報は、前記要求の送信元がオフラインで当該第 1 の通信装置に提供した情報である

請求項 1 2 に記載の通信方法。

【請求項 1 7】

前記処理の結果を送信する送信先の情報は、前記第 1 の通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための識別情報である

請求項 1 2 に記載の通信方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、他人の個人 ID 情報を不正に用いた手続を防止できる通信装置、通信システムおよびその方法に関する。

【0 0 0 2】

【従来の技術】

インターネットなどのネットワークを介して商品等の販売や代金の決済を行う電子商取引が普及している。

このような電子商取引を用いて利用者が商品等を購入する場合には、例えば、利用者が店舗や各家庭に設置されたパーソナルコンピュータなどの発注者端末装置を操作して、ネットワークを介して、商品等の販売を行うサーバ装置にアクセスを行う。これにより、サーバ装置から発注者端末装置に商品の写真、特性および価格などの情報が提供され、発注者端末装置のディスプレイに表示される。利用者は、このような情報を見ながら、購入を希望する商品等を選択し、選択した商品等の発注処理を行う。発注処理は、利用者個人を特定する個人 ID 情報、発注する商品等を指定した情報およびその決済方法等の情報を、発注者端末装置を操作して入力し、これをネットワークを介してサーバ装置に送信する。

【 0 0 0 3 】

このような電子商取引では、ネットワーク銀行などが、ネットワークを介した取引に関する決済業務を行うが、当該決済を行うに当たって、決済対象となる電子商取引の内容の正当性が認証されている必要がある。

従って、電子商取引では、このような電子商取引の内容の正当性を認証する処理を行う認証装置が用いられる。当該認証装置を用いた認証業務は、ネットワーク銀行、あるいは他の信頼性のある機関が行う。

【 0 0 0 4 】

【発明が解決しようとする課題】

ところで、上述したような認証装置では、例えば、個人ID情報を他人が不正に取得した場合に、当該他人は、その個人ID情報を用いて、認証装置に対して認証要求を出すことができ、不正な取引が行われてしまう可能性があるという問題がある。

このような他人の個人ID情報を用いてネットワークを介して行われる不正な手続（いわゆる、なりすまし）についての問題は、認証手続以外の種々の手続についても同様に存在する。

【 0 0 0 5 】

本発明は上述した従来技術の問題点に鑑みてなされ、不正に取得した他人の個人ID情報に基づいて不正な手続が行われることを回避する通信装置、通信システムおよびその方法を提供することを目的とする。

【 0 0 0 6 】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第1の発明の通信装置は、利用者を識別するための識別情報を含む要求を受信する受信手段と、前記識別情報と処理結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する送信手段とを有する。

【 0 0 0 7 】

第 1 の発明の通信装置の作用は以下になる。

例えば、利用者が他の通信装置を操作して、利用者を識別するための識別情報を含む要求を送信する。

当該要求は、受信手段で受信される。

次に、処理手段において、当該受信した要求に応じた所定の処理が行われる。

次に、送信手段によって、前記受信した要求に含まれる前記識別情報に対応する前記送信先の情報が記憶手段から読み出され、当該読み出された前記送信先の情報によって特定された送信先に、前記処理の結果が送信される。

【 0 0 0 8 】

また、第 1 の発明の通信装置は、好ましくは、前記受信手段は、暗号化された前記識別情報を含む前記要求を受信し、前記通信装置は、前記受信した要求に含まれる前記識別情報を復号する復号手段をさらに有する。

【 0 0 0 9 】

また、第 1 の発明の通信装置は、好ましくは、前記識別情報は、当該通信装置に登録された利用者に予め割り当てられた識別子である。

【 0 0 1 0 】

また、第 1 の発明の通信装置は、好ましくは、前記処理の結果を送信する送信先の情報は、前記要求の送信元がオフラインで当該通信装置に提供した情報である。

【 0 0 1 1 】

また、第 1 の発明の通信装置は、好ましくは、前記所定の結果を送信する送信先の情報は、当該通信装置が接続されるネットワークにおいて、前記利用者を一意に識別するための識別情報である。

【 0 0 1 2 】

また、第 1 の発明の通信装置は、好ましくは、前記処理は、認証処理である。

【 0 0 1 3 】

また、第 2 の発明の通信システムは、ネットワークを介して接続される第 1 の通信装置および第 2 の通信装置を有する通信システムであって、前記第 1 の通信

装置は、利用者を識別するための識別情報を含む要求を受信する第 1 の受信手段と、前記識別情報と処理の結果を送信する送信先の情報とを対応付けて記憶する記憶手段と、前記要求に応じて所定の処理を行う処理手段と、前記要求に含まれる前記識別情報に対応する前記送信先の情報を前記記憶手段から読み出し、当該読み出した前記送信先の情報によって特定された送信先に、前記処理の結果を送信する第 1 の送信手段とを有し、前記第 2 の通信装置は、前記要求を前記第 1 の通信装置に送信する第 2 の送信手段と、前記処理の結果を前記第 1 の通信装置から受信する第 2 の受信手段と、当該受信した認証処理の結果を出力する出力手段とを有する。

【 0 0 1 4 】

また、第 3 の発明の通信方法は、ネットワークを介して接続される第 1 の通信装置および第 2 の通信装置を用いた通信方法であって、利用者を識別するための識別情報を含む要求を、前記第 2 の通信装置から前記第 1 の通信装置に送信し、前記第 1 の通信装置において、前記要求に応じて所定の処理を行い、前記第 1 の通信装置は、予め用意された前記識別情報と処理の結果を送信する送信先の情報とを対応関係を参照し、前記要求に含まれる前記識別情報に対応する送信先の情報によって特定される送信先に、前記処理の結果を送信する。

【 0 0 1 5 】

【発明の実施の形態】

以下、本発明の実施形態に係わるトランザクション認証システムについて説明する。

図 1 は、本実施形態のトランザクション認証システム 1 0 1 の全体構成図である。

図 1 に示すように、トランザクション認証システム 1 0 1 では、例えば、発注者 3 1 の発注者端末装置 1 1 と、受注者 3 3 の受注者端末装置 1 5 と、ネットワーク銀行 4 0 の認証装置 5 0 とが、インターネットなどのネットワーク（通信網）を介して接続されており、発注者 3 1 と受注者 3 3 との間のトランザクション（取り引き）の正当性を認証装置 5 0 で認証する。

なお、当該ネットワークに接続されている発注者端末装置 1 1 および受注者端

末装置 1 5 の数は任意である。

【 0 0 1 6 】

本実施形態では、認証装置 5 0 が第 1 の発明の通信装置、並びに第 2 および第 3 の発明の第 1 の通信装置に対応し、受注者端末装置 1 5 あるいは不正者端末装置 5 6 が第 2 および第 3 の発明の第 2 の通信装置に対応している。

【 0 0 1 7 】

本実施形態では、例えば、発注者 3 1 および受注者 3 3 とネットワーク銀行 4 0 との間で認証を行うことに関する契約が成されている。また、発注者 3 1 と引き落とし銀行 4 2 との間では、例えば、ネットワーク銀行 4 0 によって認証された取引に関する引き落としを行う旨の契約がなされている。また、ネットワーク銀行 4 0 と保険会社 4 3 との間では、ネットワーク銀行 4 0 が係わった電子商取引によって生じた損害についての保険契約がなされている。

【 0 0 1 8 】

以下、トランザクション認証システム 1 0 1 を構成する各装置について説明する。

〔発注者端末装置 1 1〕

図 2 に示すように、発注者端末装置 1 1 は、例えば、発注者 3 1 の家庭などに設けられた、パーソナルコンピュータ、セット・トップ・ボックスあるいはゲーム機器などの装置であり、受信部 6 1、送信部 6 2、暗号化部 6 3、復号部 6 4、記憶部 6 5、制御部 6 6 および署名検証部 6 7 を有する。

なお、発注者端末装置 1 1 は、例えば、発注者 3 1 が使用する際に、発注者 3 1 の指紋等の身体的特徴から得られる情報と、予め記憶部 6 5 に予め記憶してある身体的特徴を示す情報とを比較することで、発注者 3 1 が正当な利用者であることを認証する生体認証部を有していてもよい。

【 0 0 1 9 】

ここで、受信部 6 1 が第 2 の発明の第 2 の受信手段に対応し、送信部 6 2 が第 2 の発明の第 2 の送信手段に対応している。

【 0 0 2 0 】

受信部 6 1 は、ネットワークを介して認証装置 5 0 から情報あるいは要求を受

信する。

送信部 6 2 は、ネットワークを介して認証装置 5 0 に情報あるいは要求を送信する。

また、受信部 6 1 および送信部 6 2 は、受注者 3 3 が提供する商品等の案内情報にアクセスする際に、ネットワークを介して、当該サーバ装置との間で情報あるいは要求の送受信を行う。

暗号化部 6 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 6 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 6 5 は、発注者 3 1 が作成した秘密鍵 $K_{31,S}$ などを格納する。

署名検証部 6 7 は、例えば、認証装置 5 0 が作成した署名情報を、ネットワーク銀行 4 0 の公開鍵 $K_{40,P}$ を用いて検証する。

制御部 6 6 は、発注者端末装置 1 1 内の各構成要素の処理を統括的に制御する。

【 0 0 2 1 】

制御部 6 6 は、例えば、発注者 3 1 による操作に応じて、発注情報 $a 1$ と、個人キー情報 $k 1$ （本発明の利用者を識別するための識別情報）と、個人 ID 情報 $ID 1$ （本発明の識別情報）との全体に対して暗号化を行い、もしくは個別情報毎に暗号化を行い、当該暗号化した情報を格納した認証要求 $Inf 1$ を生成する。

ここで、個人キー情報 $k 1$ および個人 ID 情報 $ID 1$ は、発注者 3 1 がネットワーク銀行 4 0 に自らを登録したときに、当該発注者 3 1 に割り当てられた固有の識別子である。例えば、個人キー情報 $k 1$ は、ネットワーク銀行 4 0 と契約した契約者（発注者 3 1）の契約番号などの個人情報を示す識別子である。また、個人 ID 情報 $ID 1$ は、発注者 3 1 の銀行口座番号などの課金に係わる情報を示す識別子である。

また、制御部 6 6 は、例えば、認証要求 $Inf 1$ を認証装置 5 0 に送信した後に、認証装置 5 0 から認証応答 $Inf 4$ を受信したときに、認証応答 $Inf 4$ に含まれる認証結果を所定の表示装置や音声出力装置を介して出力する制御を行う。

【 0 0 2 2 】

〔受注者端末装置 1 5〕

図 3 に示すように、受注者端末装置 1 5 は、サイバーモール(Cyber Mall)などに店舗を出している受注者 3 3 が使用するサーバ装置であり、受信部 7 1、送信部 7 2、暗号化部 7 3、復号部 7 4、記憶部 7 5、制御部 7 6 および署名検証部 7 7 を有する。

受信部 7 1 は、ネットワークを介して認証装置 5 0 から情報あるいは要求を受信する。

送信部 7 2 は、ネットワークを介して認証装置 5 0 に情報あるいは要求を送信する。

また、受信部 7 1 および送信部 7 2 は、発注者端末装置 1 1 からのアクセスに応じて、例えば、記憶部 7 5 から読み出した受注者 3 3 が提供する商品等の案内情報を、ネットワークを介して、発注者端末装置 1 1 に送信する。

暗号化部 7 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 7 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 7 5 は、受注者 3 3 が作成した秘密鍵 $K_{33,S}$ などを格納する。

制御部 7 6 は、受注者端末装置 1 5 内の各構成要素の処理を統括的に制御する。

署名検証部 7 7 は、例えば、ネットワーク銀行 4 0 の公開鍵 $K_{40,P}$ を用いて、認証装置 5 0 が作成した署名情報の検証を行う。

【 0 0 2 3 】

〔認証装置 5 0〕

図 4 に示すように、認証装置 5 0 は、受信部 8 1、送信部 8 2、暗号化部 8 3、復号部 8 4、記憶部 8 5、制御部 8 6、署名作成部 8 7 および課金処理部 8 8 を有する。

【 0 0 2 4 】

ここで、受信部 8 1 が、第 1 の発明の受信手段、並びに第 2 の発明の第 1 の受信手段に対応している。送信部 8 2 が、第 1 の発明の送信手段、並びに第 2 の発明の第 1 の送信手段に対応している。記憶部 8 5 が、第 1 の発明および第 2 の発

明の記憶手段に対応している。制御部 8 6 が、第 1 の発明および第 2 の発明の処理手段に対応している。

【0025】

受信部 8 1 は、ネットワークを介して発注者端末装置 1 1 および受注者端末装置 1 5 から情報あるいは要求を受信する。

送信部 8 2 は、ネットワークを介して発注者端末装置 1 1 および受注者端末装置 1 5 に情報あるいは要求を送信する。

暗号化部 8 3 は、所定の暗号鍵を用いて、情報あるいは要求を暗号化する。

復号部 8 4 は、所定の暗号鍵を用いて、情報あるいは要求を復号する。

記憶部 8 5 は、発注者 3 1 がネットワーク銀行 4 0 と契約したときに、発注者 3 1 の個人キー情報 k_1 と、個人 ID 情報 ID_1 と、発注者 3 1 のネットワーク ID_N (本発明の送信先の情報) との対応表を図 4 に示す認証装置 5 0 の記憶部 8 5 に記憶する。

ここで、ネットワーク ID_N は、発注者 3 1 がネットワーク銀行 4 0 にオフラインで登録した、当該ネットワークのユーザである発注者 3 1 をネットワーク内で一意に識別するための識別子である。

また、記憶部 8 5 は、例えば、発注者 3 1 および受注者 3 3 がネットワーク銀行 4 0 と契約をしたときに、発注者 3 1 が作成した秘密鍵 $K_{31,S}$ に対応する公開鍵 $K_{31,P}$ 、並びに受注者 3 3 が作成した秘密鍵 $K_{33,S}$ に対応する公開鍵 $K_{33,P}$ などを格納する。

制御部 8 6 は、認証装置 5 0 内の各構成要素の処理を統括的に制御する。

署名作成部 8 7 は、ネットワーク銀行 4 0 の秘密鍵 $K_{40,S}$ を用いて署名情報の作成を行う。

課金処理部 8 8 は、発注者 3 1 による取引に関する認証に対しての課金処理を行う。

認証装置 5 0 の各構成要素の詳細な処理については、後述する動作例で記載する。

【0026】

以下、トランザクション認証システム 1 0 1 の動作例を説明する。

当該動作例を開始する前提として、発注者 3 1 とネットワーク銀行 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 4 0 は、発注者 3 1 に対して、個人キー情報 k_1 および個人 ID 情報 ID_1 を発行している。

また、発注者 3 1 は、ネットワーク内で当該発注者 3 1 を識別するネットワーク ID N を、秘密が保持される環境、例えばオフラインでネットワーク銀行 4 0 に登録している。

ネットワーク銀行 4 0 は、個人キー情報 k_1 と、個人 ID 情報 ID_1 と、発注者 3 1 のネットワーク ID N との対応表を図 4 に示す認証装置 5 0 の記憶部 8 5 に記憶している。

【0027】

また、ネットワーク銀行 4 0 は、自らの秘密鍵 $K_{40,S}$ を図 4 に示す認証装置 5 0 の記憶部 8 5 に記憶すると共に、当該秘密鍵 $K_{40,S}$ に対応する公開鍵 $K_{40,P}$ を発注者端末装置 1 1 および受注者端末装置 1 5 に送信する。発注者端末装置 1 1 は、公開鍵 $K_{40,P}$ を図 2 に示す記憶部 6 5 に記憶する。受注者端末装置 1 5 は、公開鍵 $K_{40,P}$ を図 3 に示す記憶部 7 5 に記憶する。

【0028】

また、受注者 3 3 とネットワーク銀行 4 0 との間で所定の契約が結ばれ、ネットワーク銀行 4 0 は、受注者 3 3 に対して、個人キー情報 Z および個人 ID 情報 ID_2 を発行する。ネットワーク銀行 4 0 は、個人キー情報 Z および個人 ID 情報 ID_2 の対応表を図 4 に示す認証装置 5 0 の記憶部 8 5 に記憶する。

【0029】

以下、発注者 3 1 が、認証装置 5 0 に認証要求を行なった場合のトランザクション認証システム 1 0 1 の動作を説明する。

図 5 は、トランザクション認証システム 1 0 1 の当該動作を説明するための図である。

ステップ ST 1 1 :

図 1 に示す発注者 3 1 は、例えばネットワーク上の商店である受注者 3 3 に商品を発注する場合に、発注する商品名および数量などを示す発注情報 a_1 と、発注者 3 1 の個人キー情報 k_1 と、発注者 3 1 の個人 ID 情報 ID_1 とを、図示し

ない操作手段を操作して発注者端末装置 11 に入力する。なお、発注情報 a1 には、受注者 33 を特定する情報が含まれている。

次に、図 2 に示す発注者端末装置 11 の暗号化部 63 は、記憶部 65 から読み出したネットワーク銀行 40 の公開鍵 $K_{40,P}$ を用いて、発注情報 a1 と、個人キー情報 k1 と、個人 ID 情報 ID1 との全体に対して暗号化を行い、当該暗号化した情報を格納した認証要求 Inf1 (本発明の要求) を、送信部 62 からネットワークを介して、図 1 に示すネットワーク銀行 40 の認証装置 50 に送信する。

【0030】

ステップ ST12 :

図 4 に示す認証装置 50 は、発注者端末装置 11 からの認証要求 Inf1 を受信部 81 が受信すると、記憶部 85 からネットワーク銀行 40 の秘密鍵 $K_{40,S}$ を読み出し、復号部 84 において、当該秘密鍵 $K_{40,S}$ を用いて認証要求 Inf1 を復号する。

次に、認証装置 50 は、制御部 86 の制御に基づいて、上記復号した認証要求 Inf1 に格納された発注情報 a1 および個人キー情報 k1 を格納した情報 Inf1' について、記憶部 85 から読み出した自らの秘密鍵 $K_{40,S}$ を用いて署名情報 Au1 を作成する。

次に、認証装置 50 は、情報 Inf1' および署名情報 Au1 を格納した要求 Inf2 を生成する。

次に、暗号化部 83 は、図 4 に示す記憶部 85 から読み出した受注者 33 の公開鍵 $K_{33,P}$ を用いて、上記生成した要求 Inf2 を暗号化した後に、送信部 82 から、ネットワークを介して受注者端末装置 15 に送信する。

【0031】

ステップ ST13 :

受注者端末装置 15 の復号部 74 は、認証装置 50 からの要求 Inf2 を受信部 71 が受信すると、記憶部 75 から読み出した自らの秘密鍵 $K_{33,S}$ を用いて、要求 Inf2 を復号する。

次に、受注者端末装置 15 の署名検証部 77 は、上記復号した要求 Inf2 に

格納された署名情報 $Au1$ を、記憶部 75 から読み出した認証装置 50 の公開鍵 $K_{40,P}$ を用いて検証する。

【0032】

受注者端末装置 15 の制御部 76 は、署名検証部が上記検証の結果、署名情報 $Au1$ の正当性が認証されると、要求 $Inf2$ に格納された情報 $Inf1'$ を図 3 に示す記憶部 75 に記憶する。受注者 33 は、情報 $Inf1'$ 内の発注情報 $a1$ に基づいて、発注者 31 への商品等の発送予定などを示す受注確認情報 $c1$ を生成する。

次に、制御部 76 は、要求 $Inf2$ 、受注確認情報 $c1$ および自らの個人キー情報 Z を格納した応答 $Inf3$ を生成する。

次に、受注者端末装置 15 の送信部 72 は、上記生成した応答 $Inf3$ を、記憶部 75 から読み出したネットワーク銀行 40 の公開鍵 $K_{40,P}$ を用いて暗号化部 73 で暗号化した後に、送信部 72 から、ネットワークを介して認証装置 50 に送信する。

受注者 33 は、例えば、要求 $Inf2$ に格納された情報 $Inf1'$ 内の発注情報 $a1$ に基づいて、発注者 31 が発注した商品等を発注者 31 に発送したり、発注者 31 が注文したサービスを発注者 31 に提供する。

【0033】

ステップ ST14 :

認証装置 50 の復号部 84 は、受注者端末装置 15 からの応答 $Inf3$ を受信部 81 が受信すると、記憶部 85 から読み出した自らの秘密鍵 $K_{40,S}$ を用いて、 $Inf3$ を復号し、要求 $Inf1$ に格納された発注情報 $a1$ と、当該復号された $Inf3$ に格納された受注者 33 の個人キー情報 Z とを用いて、所定の取り引き履歴情報を作成し、これを記憶部 85 に格納する。当該履歴情報は、ネットワーク銀行 40 が、発注者 31 に対して決済を行う際に用いられる。

また、認証装置 50 の署名作成部 87 は、ステップ ST13 で受信した応答 $Inf3$ について、自らの秘密鍵 $K_{40,S}$ を用いて署名情報 $Au2$ を作成する。

次に、認証装置 50 の制御部 86 は、応答 $Inf3$ および署名情報 $Au2$ を格納した認証応答 $Inf4$ を作成する。

次に、認証装置 50 の暗号化部 83 は、上記作成し認証した応答 Inf 4 を、公開鍵 $K_{31,P}$ を用いて暗号化した後に、個人 ID 情報 ID 1 に対応する記憶部 85 から読み出した発注者 31 のネットワーク ID_N に基づいて送信先を特定して、送信部 82 からネットワークを介して発注者端末装置 11 に送信する。

【0034】

発注者端末装置 11 では、受信した認証応答 Inf 4 を、図 2 示す記憶部 65 から読み出した発注者 31 の秘密鍵 $K_{31,S}$ を用いて復号部 64 で復号する。

次に、発注者端末装置 11 の署名検証部 66 は、当該復号した認証応答 Inf 4 に格納された署名情報 Au 2 を、記憶部 65 から読み出したネットワーク銀行 40 の公開鍵 $K_{40,P}$ を用いて検証する。

当該検証によってその正当性が確認されると、制御部 66 は、認証応答 Inf 4 に格納されている発注情報 a 1 や取引引きの内容を示す情報に応じた出力を、発注者端末装置 11 の図示しないディスプレイやスピーカから出力する。

【0035】

以下、発注者 31 の個人 ID 1 および個人キー k 1 を不正に取得した図 1 に示す不正者 55 が自らの端末装置である不正者端末装置 56 を用いて、認証装置 50 に認証要求を送信した場合のトランザクション認証システム 101 の動作を説明する。

ここで、不正者端末装置 56 の構成は、例えば、図 2 に示す発注者端末装置 11 と同じである。

図 6 は、トランザクション認証システム 101 の当該動作を説明するための図である。

ステップ ST 21 :

図 1 に示す不正者 55 は、受注者 33 に商品を発注する場合に、発注する商品名および数量などを示す発注情報 a 1 と、不正に取得した発注者 31 の個人キー情報 k 1 と、不正に取得した発注者 31 の個人 ID 情報 ID 1 とを、図示しない操作手段を操作して不正者端末装置 56 に入力する。

次に、不正者端末装置 56 の図 2 に示す暗号化部 63 は、記憶部 65 から読み出したネットワーク銀行 40 の公開鍵 $K_{40,P}$ を用いて、発注情報 a 1 と、個人キ

ー情報 k_1 と、個人 ID 情報 ID_1 との全体に対して暗号化を行い、当該暗号化した情報を格納した認証要求 Inf_1 を、送信部 62 からネットワークを介して、図 1 に示すネットワーク銀行 40 の認証装置 50 に送信する。

【0036】

ステップ ST22 :

図 4 に示す認証装置 50 は、不正者端末装置 56 からの認証要求 Inf_1 を受信部 81 が受信すると、当該認証要求 Inf_1 について、前述したステップ ST12 と同様の処理を行なう。

【0037】

ステップ ST23 :

ステップ ST23 の処理は、前述したステップ ST13 の処理と同じである。

【0038】

ステップ ST24 :

ステップ ST24 の処理は、前述したステップ ST14 の処理と同じである。

すなわち、不正者 55 が不正者端末装置 56 を用いて、認証要求 Inf_1 を認証装置 50 に送信した場合でも、その応答である認証応答 Inf_4 は、認証装置 50 の記憶部 85 に記憶されている発注者 31 のネットワーク ID_N に基づいて、発注者端末装置 11 に送信される。

これにより、発注者 31 は、受信した認証応答 Inf_4 に基づいて、自らが個人 ID 情報 ID_1 を用いた不正な認証要求が行なわれたことを知ることができ、その旨をネットワーク銀行 40 などに通知する。

【0039】

以上説明したように、トランザクション認証システム 101 によれば、認証装置 50 は、発注者 31 がネットワーク銀行 40 にオフラインで登録したネットワーク ID_N によって指定された送信先に、認証応答 Inf_4 を送信するため、例えば、発注者 31 の個人情報 ID_1 を不正に取得した者が当該個人情報 ID_1 を用いて認証装置 50 に認証要求を行なった場合に、認証装置 50 に登録されたネットワーク ID_N に基づいて認証装置 50 から発注者端末装置 11 に送信された認証応答 Inf_4 によって、発注者 31 は自らの個人情報 ID_1 を用いた不

正な取引が行なわれることを知ることができる。

そのため、トランザクション認証システム 1 0 1 によれば、他人の個人 I D 情報を用いた不正な取引を効果的に抑制できる。

【 0 0 4 0 】

上述したように、トランザクション認証システム 1 0 1 によれば、電子商取引の信頼性を向上でき、当該認証機関と契約する契約者（取引引き者）の数を増やし、各契約者に課す会費などを費用を低額にでき、電子商取引をさらに普及させることが可能になる。

【 0 0 4 1 】

本発明は上述した実施形態に限定されない。

例えば、上述した実施形態では、本発明の処理手段が行う処理として認証処理を例示したが、その他、課金処理などの処理を行う場合にも本発明は適用可能である。

【 0 0 4 2 】

また、上述した実施形態では、ネットワーク銀行 4 0 が、認証装置 5 0 を用いて、トランザクション（取引引き）の認証業務を行う場合を例示したが、ネットワーク銀行 4 0 とは別の機関が、認証装置 5 0 を用いてトランザクションの認証業務を行うようにしてもよい。

【 0 0 4 3 】

【発明の効果】

以上説明したように、本発明によれば、不正に取得した他人の識別情報（個人 I D 情報）に基づいて不正な手続が行われることを回避する通信装置、通信システムおよびその方法を提供できる。

【図面の簡単な説明】

【図 1】

図 1 は、本発明の実施形態のトランザクション認証システムの全体構成図である。

【図 2】

図 2 は、図 1 に示す発注者端末装置の構成図である。

【図 3】

図 3 は、図 1 に示す受注者端末装置の構成図である。

【図 4】

図 4 は、図 1 に示す認証装置の構成図である。

【図 5】

図 5 は、発注者が認証装置に認証要求を行なった場合のトランザクション認証システムの動作のフローチャートである。

【図 6】

図 6 は、不正者が認証装置に認証要求を行なった場合のトランザクション認証システムの動作のフローチャートである。

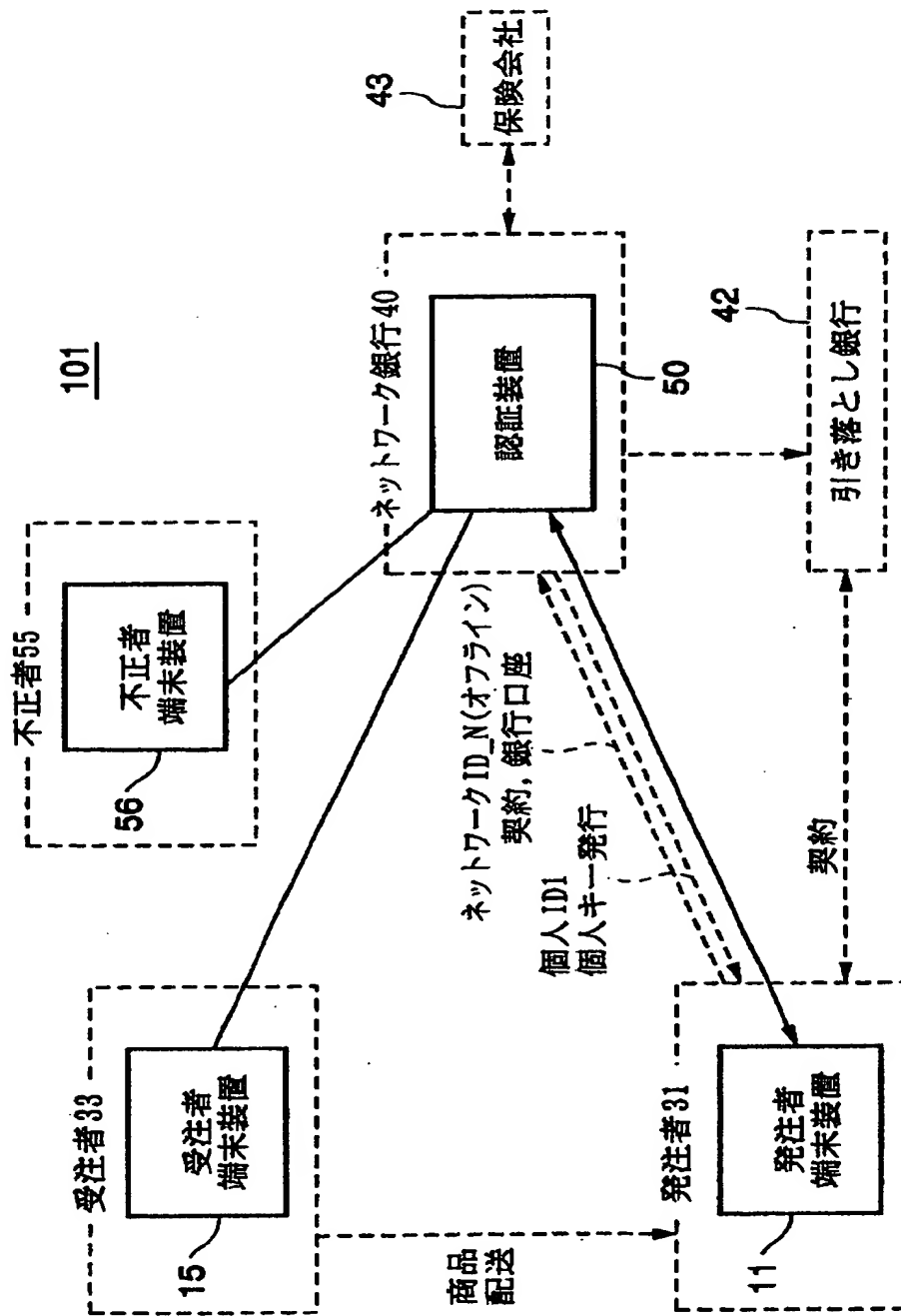
【符号の説明】

1 … トランザクション認証システム、 1 1 … 発注者端末装置、 1 5 … 受注者端末装置、 3 1 … 発注者、 3 3 … 受注者、 4 0 … ネットワーク銀行、 5 0 … 認証装置、 6 1, 7 1, 8 1 … 受信部、 6 2, 7 2, 8 2 … 送信部、 6 3, 7 3, 8 3 … 暗号化部、 6 4, 7 4, 8 4 … 復号部、 6 5, 7 5, 8 5 … 記憶部、 6 6, 7 6, 8 6 … 制御部、 6 7, 7 7 … 署名検証部、 8 7 … 署名作成部、 8 8 … 課金処理部、 a 1 … 発注情報、 k 1 … 発注者 3 1 の個人キー情報 k 1、 I D 1 … 発注者 3 1 の個人 I D 情報、 I D _ N … ネットワーク I D、 A u 1, A u 2 … 認証装置の署名情報、 Z … 受注者の個人キー情報、 I n f 1 … 認証要求、 I n f 4 … 認証応答

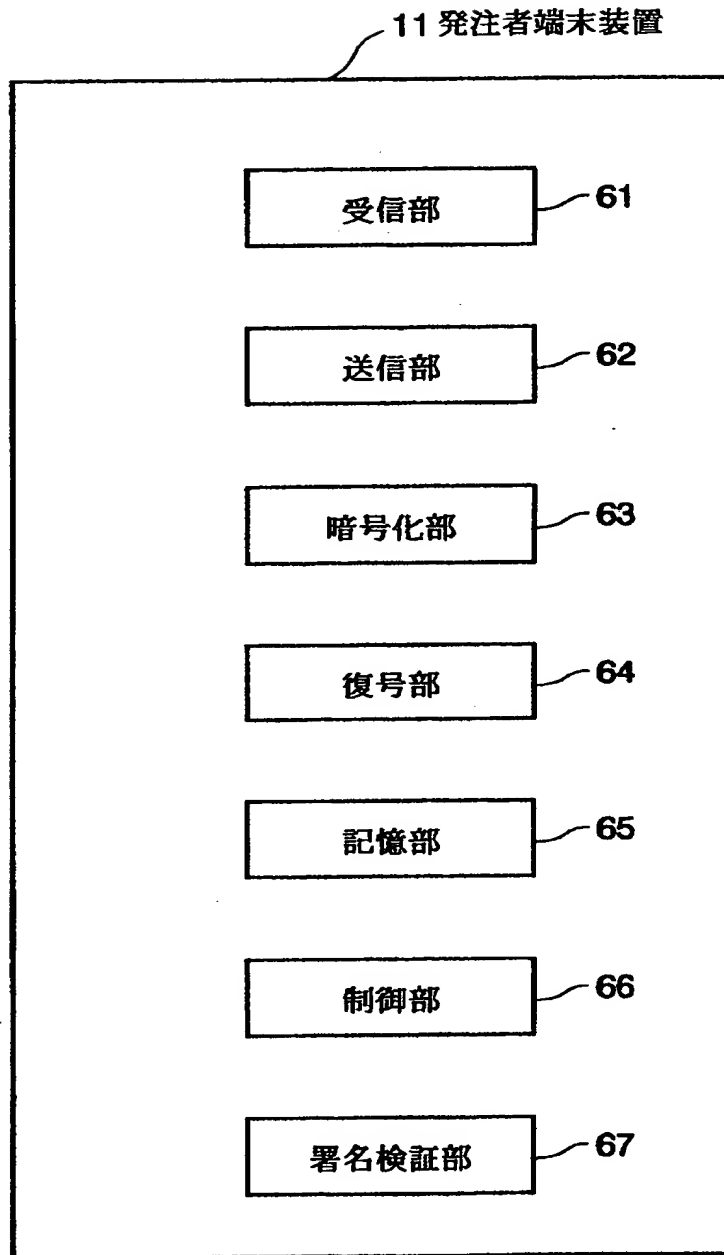
【書類名】

図面

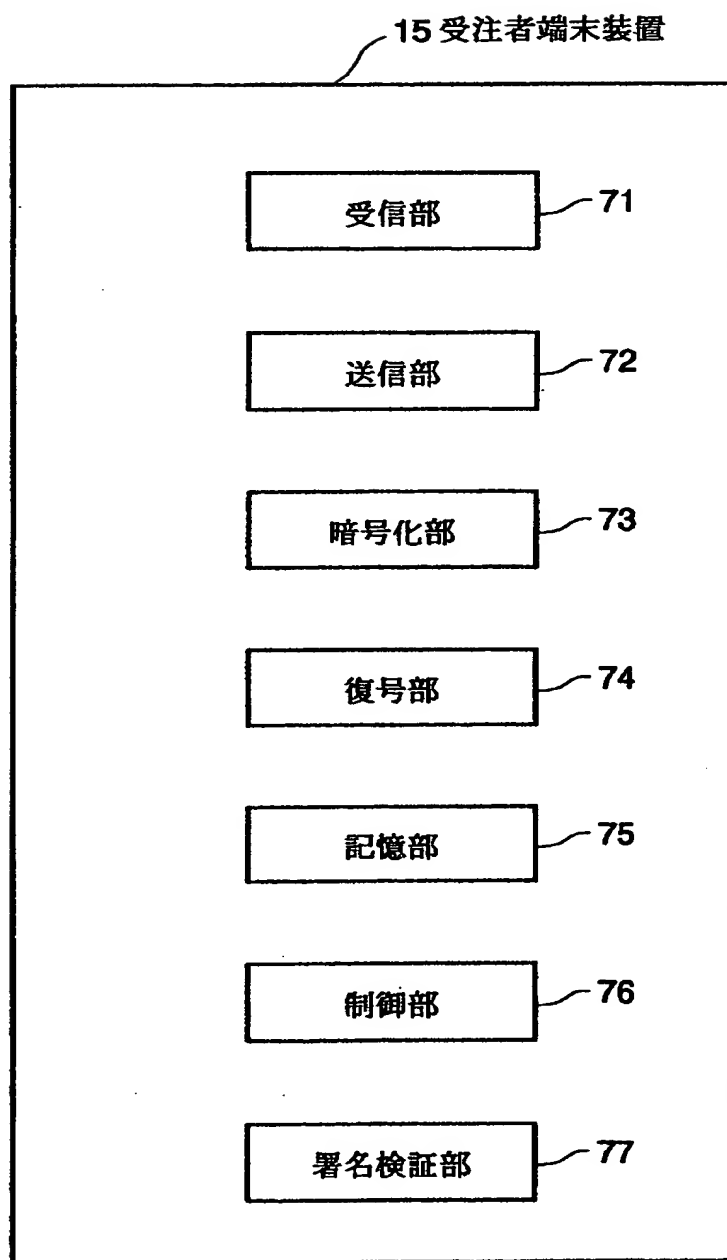
【図 1】



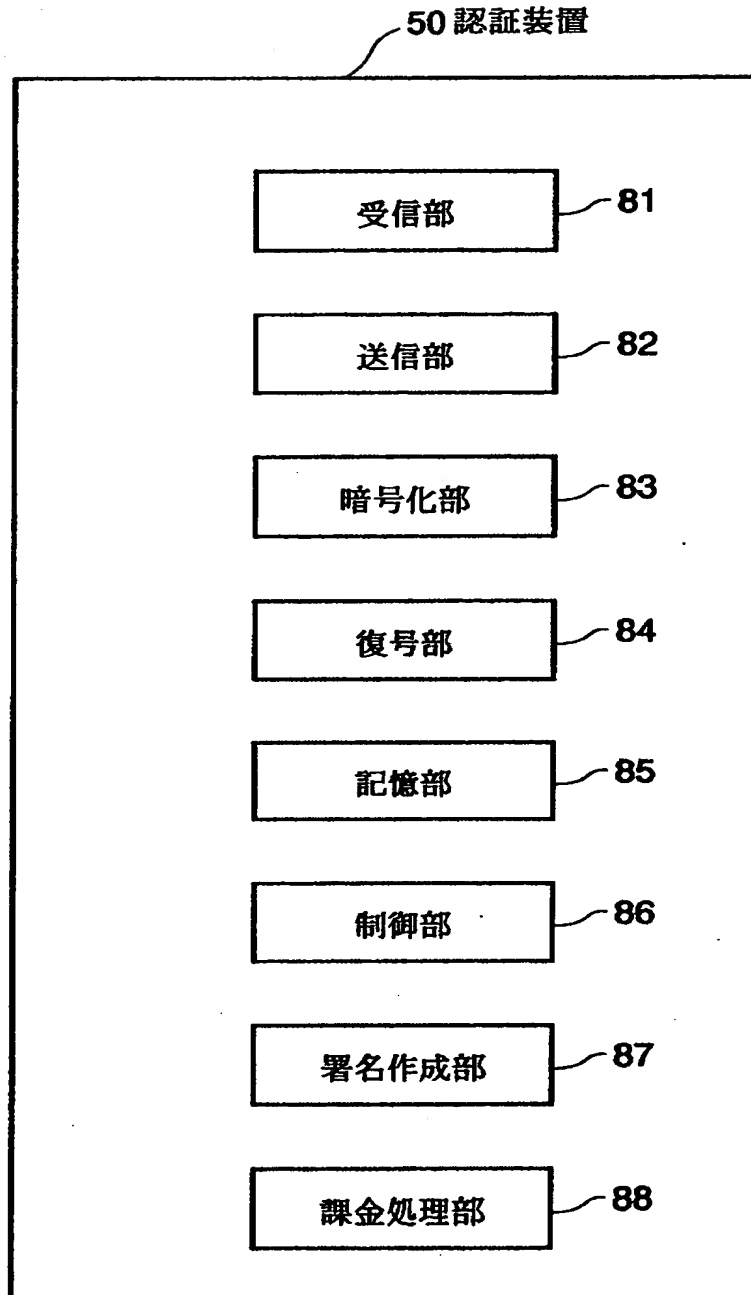
【図 2】



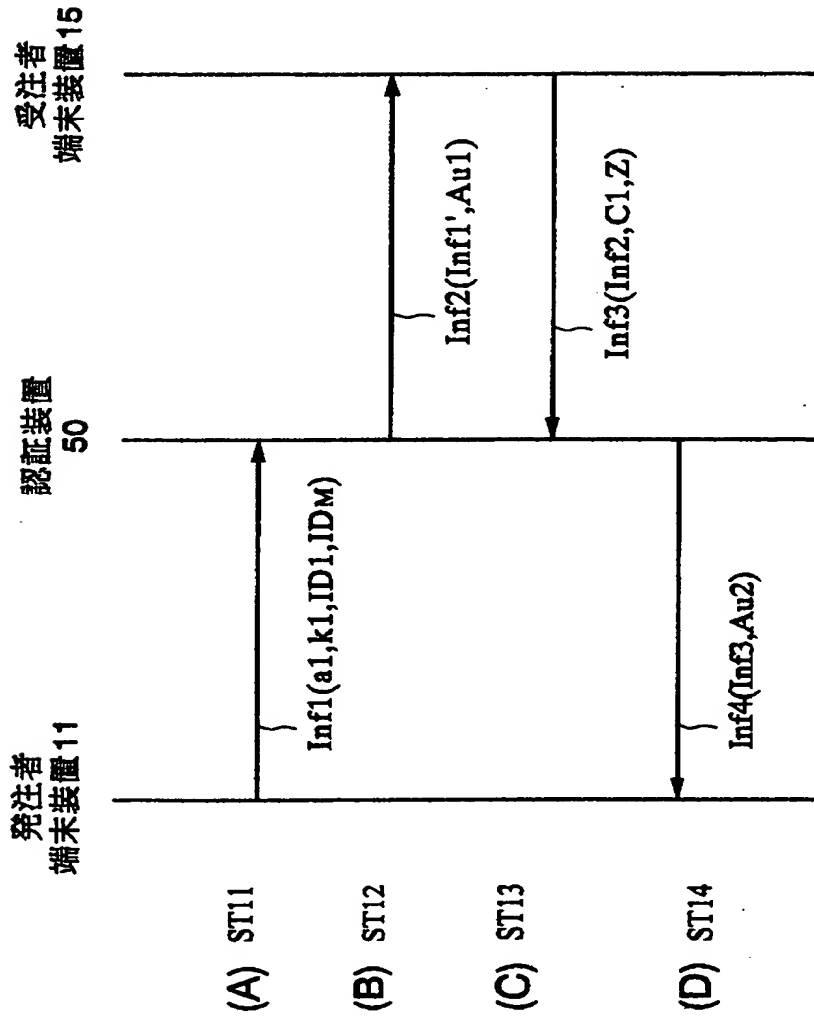
【図 3】



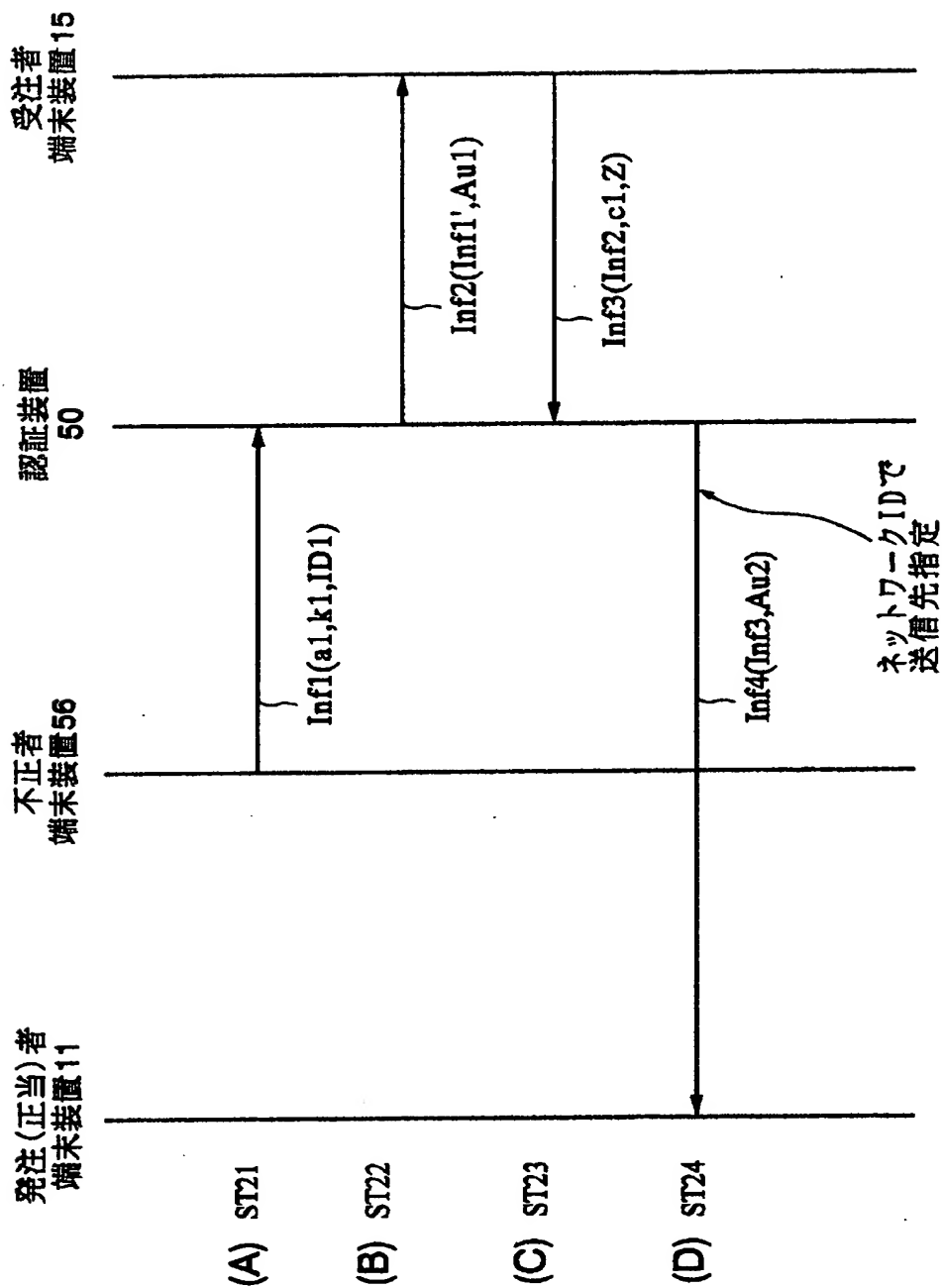
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 不正に取得した他人の個人 I D 情報に基づいて不正な手続が行われることを回避する通信装置を提供する。

【解決手段】 認証装置 5 0 は、端末装置 1 1 などから利用者の個人 I D 情報を含む要求を受信し、当該要求に応じた認証処理を行う。認証装置 5 0 は、認証処理の結果を、予め保持している個人 I D 情報と処理結果を送信する送信先の情報であるネットワーク I D __ N との対応関係に基づいて、端末装置 1 1 に送信する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社

This Page Blank (uspto)